The Internet, The Oppressor: Human Security in Cyberspace

By
William Yates Jordan

Submitted to
Central European University
School of Public Policy

In partial fulfilment for the degree of Master of Arts in Public Policy

Supervisor: Cameran Ashraf

Budapest, Hungary

2018

CEU eTD Collection

Author's Declaration

I, the undersigned, William Yates Jordan, hereby declare that I am the sole author of this thesis. To the best of my knowledge this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted as part of the requirements of any other academic degree or non-degree program, in English or in any other language.

This is a true copy of the thesis, including final revisions.

Date: 15 June 2018

Name: William Yates Jordan

Signature: ……..

CEU eTD Collection

Abstract

The rapid growth and assimilation of digital technologies has drastically altered the ways in which the world functions. As the prominence of cyberspace has grown, so too has the importance of ensuring security for its users. While security may be a goal for all, the question of who or what cybersecurity is supposed to protect has resulted in dramatically different approaches and outcomes for individuals in cyberspace. The current traditional approach has made states the purveyors of cybersecurity, but this has resulted in a decidedly less secure space for individuals. To rectify this problem, this thesis argues that a paradigmatic shift from traditional to human security is needed in cyberspace. In order to highlight the failings of traditional security in cyberspace and the need for a new human-centric approach, this thesis will examine the use of advanced censorship and surveillance technology in the facilitation of human rights violations around the world. By looking at three cases where technology from Blue Coat Systems, Hacking Team, and Netsweeper were used in human rights violations, this thesis will highlight the urgent need to establish a human security paradigm in cyberspace and provided recommendations for its implementation.

CEU eTD Collection

Acknowledgements

I would like to express my sincere gratitude to my supervisor Cameran Ashraf, and academic writing instructor Sanjay Kumar, for their instrumental help in the writing of this thesis. I would also like to thank my partner Emily for her thoughtful insights, tireless editing, and moral support throughout the duration of this writing process. Lastly, I would like to thank all my friends and colleagues who have made this past year at CEU amazing.

CEU eTD Collection

Table of Contents

Introduction **1**

Chapter 1: Literature Review, Theoretical Background, and Methodology **4**

1.1 Human Security: An Emerging Paradigm 5

1.2 Security Paradigms in Cyberspace 10

1.3 Methodology 14

Chapter 2: Case Studies in Censorship, Surveillance and Human Rights **18**

2.1 Blue Coat Systems: Censorship, Surveillance, and the Arab Spring 19

2.2 Hacking Team 21

2.3 Netsweeper 24

Chapter 3: Analysis and Recommendations **27**

3.1 Borderless Rights and Ramifications 27

3.2 Recommendations 31

Conclusion **35**

Reference List **37**

CEU eTD Collection

List of Tables

Table 1: Traditional and Human Security

List of Figures

Figure 1: Hacking Team Brochure

Figure 2: Email with Spyware Sent to the Managing Director of ESAT

List of Abbreviations

UNDP - United Nations Development Program

HDR - Human Development Report

FBI - Federal Bureau of Investigation

U.S. - United States of America

U.A.E. - United Arab Emirates

GB - Gigabyte

LGBTQI+ - Lesbian, Gay, Bisexual, Transgender, Queer or Questioning, Intersex and other Identities and Orientations

DPI - Deep Packet Inspection

USD - United States Dollar

ESAT - Ethiopian Satellite Television Service

NATO - North Atlantic Treaty Organization

TFVAW - Technology Facilitated Violence Against Women

CEU eTD Collection

Introduction

The rapid growth and assimilation of digital technologies into society has drastically altered the ways in which the world functions. The Internet has become so important that in 2016 the United Nations Human Rights Council passed a non-binding resolution that condemned the prevention or disruption of access to information online by states (UNGA 2016). The indispensability of the Internet has also elevated the importance of security in cyberspace. Just as in the physical world, differing designations of the object of security in cyberspace has resulted in dramatically different policies and beneficiaries. The traditional security paradigm that currently defines cyberspace puts the state and its integrity as the primary beneficiary of security. This type of security, with similar conceptual foundations to those present in international security during the Cold War, has resulted in more insecurity for individuals (UNDP 1994, 22). From freedom of expression violations to physical violence, the traditional security paradigm in cyberspace has placed the security of humans, secondary to that of the state.

In order to rectify these shortcomings, a complete rethinking of the approach to security in cyberspace is needed. To provide individuals with security that is relevant to them, a transition to a human security paradigm must be adopted. This thesis is comprised of three chapters, which bridge the conceptual gap between the core concepts of human security and the protection of human rights in cyberspace. In so doing, this thesis will provide the rationale behind why implementing a human security paradigm in cyberspace will lead to improved holistic security for all, and the methodological approach that must be taken to complete the transition.

In Chapter 1, the conceptual differences between human and traditional security will be reviewed to establish the human security framework, as well as to provide the core arguments and approaches needed to transition to a human security paradigm in cyberspace. Human security, which has deep philosophical roots (Taylor 2004, 16), mandates individuals have 'freedom from

CEU eTD Collection

fear' and 'freedom from want' (UNDP 1994, 22). More specifically, the 1994 United Nations Development Program Human Development Report detailed how humans not only required protection from violent external aggression but chronic and sudden threats such as poverty, disease and natural disasters. After examining and analyzing these components of human security, a conceptual look at their application in cyberspace will be completed to highlight how differing approaches to security in cyberspace lead to vastly different outcomes.

Following the conceptual examination of human security, a case study analysis is conducted in Chapter 2 that explores one of the darkest components of cyberspace, advanced dual-use censorship and surveillance technology. This technology, developed and maintained by cybersecurity firms around the world, while having legitimate uses, is frequently deployed by governments to facilitate human rights violations (Deibert 2016). Chapter 2 will examine three influential cases from the past ten years of cybersecurity firms based in North America and Europe providing advanced censorship and surveillance technology used in the facilitation of human rights violations by oppressive regimes. The actions of these three cybersecurity firms, Blue Coat Systems, Hacking Team, and Netsweeper, exemplify the failings of traditional security in cyberspace to protect individuals, as the services provided by these companies actively eroded the security of civilians. By studying these failures, this thesis will provide a detailed analysis of the violations of human security perpetuated by these technologies, and illustrate how the interdependence of the pillars of human security mean that once one aspect of human security is attacked, so too are all the rest. This interdependence will demonstrate that without human security fully protected in cyberspace, it will never be achieved in the physical realm.

Finally, in Chapter 3, an analysis of the three cases studies from Chapter 2 will provide the foundations for the conclusions and recommendations of how human security should be implemented in cyberspace. As technology continues to advance and shape our society, the exact tools and methods needed to ensure human security will likely evolve, however, the core aspects

CEU eTD Collection

that must be protected will likely remain. From freedom of expression, to freedom from discrimination, and the right to privacy, this thesis will provide conceptual recommendations and approaches that policy-makers, cybersecurity firms and governments must consider when addressing security in cyberspace. If the international community seeks to protect human rights and ensure human security for all, then the principles that guide states in the physical realm must also be respected in cyberspace.

CEU eTD Collection

Chapter 1: Literature Review, Theoretical Background, and Methodology

In 2016, the United States Federal Bureau of Investigation (FBI) filed an application to compel Apple Inc. (Apple) to provide backdoor access to the encrypted iPhone of the attacker responsible for the 2015 mass shooting in San Bernardino, California (Selyukh 2016). The order stated that the FBI had explored all other possible methods of gaining access to the phone and demanded that Apple provide 'reasonable technical assistance' to help the FBI accomplish this task (Kharpal and Roth 2016; Cardozo and Crocker 2018). Publicly, the FBI framed their application as a one-time request but, Tim Cook, the CEO of Apple, stated that providing a backdoor into one phone would create, "a master key, capable of opening hundreds of millions of locks (Kharpal and Roth 2016)." Cook also warned that it could create a dangerous international precedent for other countries, particularly with authoritarian governments, to make the same request for backdoors into phones.

This public battle between the FBI and Apple illustrated the ideological divide between their concepts of security. The FBI, whose goal is to protect Americans from threats such as domestic terrorism, was willing to sacrifice the civil liberties of millions of Americans and potentially many more around the globe to do so. This approach comes in stark contrast with that of Apple's, whose approach valued the security of its users from malevolent actors over a one-off request. The ideological disparity between the two parties in 2016 has recently become even more stark as a March 2018 report from the Department of Justice's Office of the Inspector General, revealed that the FBI's main goal in the legal proceedings against Apple was not to create a backdoor in the San Bernardino shooter's phone, but to set a legal precedent that would require Apple to provide similar access in the future (Cardozo and Crocker 2018). The report revealed that the FBI had not consulted its own technology experts about other possible avenues of entry into the iPhone before testifying there was no other way (Cardozo and Crocker 2018). Additionally, it found that senior officials within the FBI were frustrated when the agency was able to unlock

CEU eTD Collection

the phone through a third party and had to withdraw their case against Apple (Cardozo and Crocker 2018). Essentially, the FBI sought a way to ensure that the encryption standards, designed to keep the many millions of iPhone users safe, be permanently weakened and were neither concerned with the implications of such a decision or the veracity of their claims.

It is with this contrast in mind that Chapter 1 will approach the important conceptual and practical differences of traditional and human security paradigms. The traditional approach to security, as seen in use by the FBI, has consistently valued national security over civil liberties. On the other hand, Apple's human security approach places value in individual security and liberties, even when at times it comes into contrast with law enforcement desires. The immense harm that could come from governments having the ability to monitor and control information and communications at will cannot be understated. For a society to succeed, the expression of dissent and ability to hold those in power to account is necessary. In order to ensure the protection of human rights, a transition away from traditional to human security in cyberspace is of the utmost importance.

1.1 Human Security: An Emerging Paradigm

As seen in the example above, the conceptualization of security in the physical and digital realm has critical implications for its implementation and beneficiaries. Many approaches to security exist, however, two dominant paradigms, traditional and human security, represent distinctly diverging ways in which security can be manifested. In the broadest of terms, traditional security is state-centric and concerned with issues such as territorial integrity and political sovereignty (Attina 2016, 175; Taylor 2004, 16; UNDP 1994, 22). Conversely, human security is centered on the individual, based on the principles of 'freedom from fear' and 'freedom from want', with the primary goal of ensuring people's ability to meet their essential needs. ("Human Security: A Stronger Framework for a More Secure Future | Human Development Reports" n.d., 1; UNDP 1994, 24). The conceptual differences that undergird these two security paradigms

CEU eTD Collection

provide insight into the key benefits that human security provides for individuals over the traditional approach.

1.1.1 Philosophical Underpinnings

The practical manifestation of human security did not begin to emerge until the end of the Cold War; however, its modern philosophical underpinnings began in the eighteenth century with Montesquieu, Adam Smith and Condorcet (Taylor 2004, 16). These liberal Enlightenment philosophers believed individual security was an important part of the societal contract with the state that ensured the protection of individuals' rights over that of the state's security (Taylor 2004, 16). Contrarily, from a realist perspective, security of the state extended downwards to individuals (Liotta and Owen 2006, 40). Thinkers, such as Thomas Hobbes, believed that security for individuals, whether from internal or external threats, was the ultimate responsibility of the state, and that individuals should sacrifice their personal liberties for security (Taylor 2004, 16). This realist approach to security has historically taken precedence over the individualist approach, peaking during the Cold War when international security was defined as a balance of power between dominant states (Taylor 2004, 16). However, by the end of the Cold War, many had realized that a state-centric focus for security was not adequately covering the needs of the people states were supposed to protect (UNDP 1994, 22). Threats, such as disease, crime, hunger, repression and environmental degradation, which greatly affected people at the time, were not being addressed (UNDP 1994, 22).

Taylor Owen, in *Challenges for Defining and Measuring Human Security*, outlines the distinct differences between what constitutes a threat when the object of security is changed, as seen in table 1 below (Taylor 2004, 17).

CEU eTD Collection

Table 1. Traditional and Human Security

Type of Security	Referent Object	Responsibility to Protect	Possible Threats
Traditional Security	The State	The Integrity of the State	Interstate War, Nuclear Proliferation, Revolution
Human Security	The Individual	The Integrity of the Individual	Disease, Poverty, Natural Disaster, Violence, Landmines, Human Rights Abuses

When the state is the referent object, as in the case of the traditional security we see that threats to it are of a military nature. Countering this, with the individual as referent object, the security provided by the military, or from violence in general, is only a portion of what people require to be secure in their lives. This widening of the concept of security also fundamentally changes the approach from one that is defensive to one that is integrative and proactive (UNDP 1994, 24). Human security recognizes that individuals do not solely need defensive protection from external armed aggression, but require a proactive and interdependent approach that incorporates all aspects of life that are needed to feel secure (UNDP 1994, 24).

1.1.2 Human Security in Practice

Beyond the conceptual differences between human and traditional security, there are clear differences in the ranges of policies required to ensure the successful implementation of a human security paradigm. In 1994, the United Nations Development Program, in consultation with Mahbub ul Haq, released the Human Development Report (HDR), which is widely considered to be the first comprehensive attempt to define what human security meant in practice (Liotta and Owen 2006, 38; Chiarello 2015; Bajpai 2000, 10). After highlighting the failings of traditional security during the Cold War, which sought only to protect individuals from violent disruptions to their lives (UNDP 1994, 22), the HDR specified what human security meant beyond 'freedom

CEU eTD Collection

from fear', and 'freedom from want'. First, it emphasized the universality and interdependence of human security, as all people rich or poor face threats to human security (UNDP 1994, 22). Second, it asserted that human security is centered on people, concerned with their ability to freely make choices and meet their most essential needs (UNDP 1994, 23). To do this, the HDR argues that human security mandates protection from chronic threats, including hunger, ethnic or political oppression, disease and environmental degradation (UNDP 1994, 23). Additionally, human security necessitates safety from harmful and unexpected disruptions to people's lives, such as natural disasters and violence (UNDP 1994, 23). When put together, these two main aspects of human security illustrate the shortcomings of traditional security and its inability to ensure the holistic security of individuals.

To bridge these two main aspects of human security, the 1994 HDR outlines seven categories that comprise human security: economic security, food security, health security, environmental security, personal security, community security and political security (UNDP 1994, 24, 25).

The first four categories, economic, food, health and environmental security are all distinct to human security. Economic security requires people have the ability to earn a basic income, and when that is not possible, have access to a publicly funded safety net (UNDP 1994, 25). Health and food security are defined by people's ability to economically and physically access basic levels of both (UNDP 1994, 27, 28). This entails access to health services, clean water and nutrient sufficient food (UNDP 1994, 27, 28). Underpinning food, health and economic security is environmental security. Environmental security means that individuals need a healthy environment to adequately provide for themselves (UNDP 1994, 29). A lack of clean water, desertification, air pollution and deforestation to name a few, greatly affect the environment's ability to support people, and people's ability to support themselves (UNDP 1994, 29).

CEU eTD Collection

The final three aspects of human security as detailed in the 1994 HDR: personal, community and political security, both incorporate and come in direct contrast with facets of traditional security. Furthermore, these three types of security have the most direct applications in cyberspace and will be discussed in more detail in section 1.2.

Similar to traditional security, personal security mandates individuals be protected from physical violence. This can mean protection from other states, individuals or groups but is also expanded to include threats from the state itself, and threats to the self (UNDP 1994, 30). Community security is based upon the concept of individual's security within particular groups such as a family, community, organization or ethnic group (UNDP 1994, 31, 32). This demands security from oppressive practice being used within the group, as well as protection from violence and discrimination due to affiliation with a group (UNDP 1994, 32). Lastly, political security strays the farthest from concepts of traditional security and in many ways comes in direct conflict with it. Political security demands people be able to live in a society that protects their basic human rights, which are often violated by the states themselves (UNDP 1994, 32). State sponsored oppression in the form of torture, police violence, and curtailed freedom of expression, to name a few; all constitute attacks on political security (UNDP 1994, 33). These three facets of human security signify why a paradigmatic shift away from traditional security is needed to both reconfigure the priorities of security and greatly expand its scope.

It is also important to recognize that the considerable interdependence of the elements of human security means a threat to one is a threat to all (UNDP 1994, 33). A failure to provide environmental security will likely lead to failings in food security, just as a failure to protect community and political security will inevitably lead to a loss of personal security. For human security to be realized it is imperative that all of its facets detailed above be protected.

Human security is a concept that has continued to grow and morph as it has been implemented over time (Gomez and Gasper, n.d., 2). The emphasis on national ownership of

CEU eTD Collection

policies and programs pertaining to human security is an important one, as different local and regional needs must be addressed to ensure human security is achieved worldwide. Thus, even though some aspects the UN has used to define human security do not translate into cyberspace, the core concepts of 'freedom from fear' and 'freedom from want' are extremely important. The shift in policies and beneficiaries that come from switching the referent object of security from the state to the individual will have a similarly massive impact on the way security is conceptualized in cyberspace as it has been in the physical realm. The growing importance of digital technologies in everyday life has extended the interdependence that defines the concepts of human security into cyberspace. This newfound indispensability of the Internet means that without the principles of human security being respected in cyberspace, human security in the physical realm will never be realized.

1.2 Security Paradigms in Cyberspace

The world's emergence into the digital age has greatly altered its informational and operational landscape. Internet penetration rates have risen at a rapid pace over the past thirty years, creating an international landscape that has become extremely dependent upon cyberspace ("Internet Growth Statistics 1995 to 2017 - the Global Village Online" n.d.). The growing importance of the Internet in people's daily lives around the world has only strengthened the need for adequate protections of individual security and human rights online. Unfortunately, the pace of change brought about by the Internet has not been matched by legislation and policies designed to deal with these new technologies. As such, old ideas have been too quickly recycled to deal with new problems.

In particular, the conflation of cybersecurity with state security, or traditional security, has led to a militarization of cyberspace that has resulted in a far less secure space for civilians (Dunn Cavelty 2014, 2). By consistently invoking images of anarchy and crime in cyberspace as issues of national security, states are able to push forward the idea of the military as its logical defender

CEU eTD Collection

(Dunn Cavelty 2014, 8). Ron Deibert, director of the Citizen Lab at Toronto University, has written much on the dark side of cyberspace that states use to justify their security policies. In Deibert's piece, *The Growing Dark Side of Cyberspace (...and What to Do about It)*, he asserts that while an ominous side of the Internet exists, it is the reactions and responses to this dark side that can be a far more sinister (Deibert 2012, 261). Just as in the physical realm, when the military defines security policy, individuals and their civil liberties can suffer. In order to avoid this potential violation of civil liberties, the approach to security in cyberspace must transition from traditional to human-centric.

1.2.1 Objects and Threats

The first step in transitioning cybersecurity to a human security paradigm is addressing the referent object of security in cyberspace. The question of who, or what, security is supposed to protect is further complicated in cyberspace. The rise of cloud computing and social networking has put a massive amount of personal data online (Deibert 2012, 263). This trove of data and its rising profitability has made the referent object of security in cyberspace the uninterrupted flow of information itself, and its protection a matter of national security (Dunn Cavelty 2014, 7). When the flow of information is the referent object, then humans are considered a threat, as vulnerabilities or hackers, to the system (Dunn Cavelty 2014, 7). This creates a clear conflict of interest in the desired outcomes of a secured cyberspace. Issues critical for human security in cyberspace, such as freedom of expression, privacy and anonymity, are subverted in the name of state security (Dunn Cavelty 2014, 4). So long as the flow and access to data is the referent object of security, then individuals will be operating in a space that is less secure for them by design (Dunn Cavelty 2014, 3).

CEU eTD Collection

1.2.2 Motives and Incentives

The conflation of state security with cybersecurity has in many ways come about due to a failure to adequately define cybersecurity. The few definitions and concepts associated with cybersecurity today have largely been driven by organizations with vested interests in cybersecurity technology (Kovacs and Hawtin 2013, 3). These companies and their lobbying efforts are behind much of the information that has resulted in cyberspace being discussed as a chaotic dangerous space that is in need of urgent protection (Dunn Cavelty 2014, 2; Kovacs and Hawtin 2013, 3). This language and tone has been used by governments, both authoritarian and democratic, to push for the militarization of cyberspace (Dunn Cavelty 2014, 8).

The militarization of cyberspace has had dire consequences for the security of individuals operating within it, as the motives and incentives for the state differ greatly from individual users. Unfortunately, just as in the physical realm, what is in the military's best interest often puts the people it is designed to protect in harm's way. Three prime examples of this are the mass surveillance practices and anti-encryption stances of states, the Stuxnet attack, and the zero-day market.[1]

With the state as the purveyor of security in cyberspace, control over the flow of information has become an area of conflict between individual civil liberties and state security. Due to the rapid advancement of digital technologies and their immense profitability, companies often push out updates that emphasize accessibility and leave security chronically 'underproduced' (Dunn Cavelty 2014, 4). This insecurity for individuals has ironically been considered a benefit for traditional security in cyberspace, as the access to user's information is considered a necessity by law enforcement and military agencies alike to secure cyberspace, as made evident by the San Bernardino case.

CEU eTD Collection

[1] A zero-day is an exploit/weakness in a software that is unknown to its creator and users and has not been previously exploited.

Incidents similar to the one that played out in San Bernardino have led many governments to attempt to curtail and weaken encryption technologies (Dunn Cavelty 2014, 10). One reason this is problematic is due to the mass surveillance practices employed by governments around the world. The Snowden leaks in 2013 showed that it was not just authoritarian regimes that were spying on their citizens but democratic governments as well (Reitman 2016). Governments' attempts to find exploits in encryption standards also greatly weakens them, and potentially leaves individuals open to attacks from malevolent actors and destroys confidence in the system as a whole (Dunn Cavelty 2014, 10). For people to be secure in cyberspace, governments need to strengthen and not weaken encryption standards.

The Stuxnet attack and the zero-day market also highlight the direct risk that state sponsored cybersecurity can present for individuals. Due to the lack of transparency pertaining to cyber technologies and practices, it is not known how large the zero-day market is; however, the entrance of governments into the market has drastically expanded its size and its prices (Dunn Cavelty 2014, 8). By entering the market, governments are using taxpayer money to prop up and expand a market selling software vulnerabilities that may affect millions of its own citizens. Instead of turning over these exploits to companies so that they can be fixed, governments are purchasing them for use in offensive cyber weapons, such as the Stuxnet virus (Zetter 2011).

Stuxnet, was created by the United States (U.S.) to damage centrifuges in Iran's nuclear facility in Natanz, by infecting their control mechanisms (Siemens PLCs) with a piece of malware (Zetter 2011). This malware used not just one, but four zero-day exploits to pull off the attack (Zetter 2011). Not only did this attack rely on zero-days that until patched, leave anyone operating the software at risk, but the attack did not remain confined to its target and infected computers all over the world, including Iran, Indonesia, India and the U.S. (Zetter 2011). What these examples, of the zero-day market, Stuxnet, and the fight of over encryption show is that when cybersecurity

CEU eTD Collection

is approached from a traditional security perspective it often actively leads to insecurity for individuals.

1.2.3 Physical Consequences

The failures of traditional cybersecurity to protect individuals in cyberspace, and the need to move toward a human security paradigm are clear. Ending mass surveillance programs, ensuring freedom of expression online, and strengthening encryption and privacy protections online, are all reasons in and of themselves to change the approach of security in cyberspace. However, the need for human security in cyberspace is not confined within its borders. The physical and often negative ramifications, of failing to promote human security in cyberspace, has resulted in many grave human rights violations (Deibert 2012, 271). Oppressive regimes around the world have enlisted the help of advanced censorship and surveillance technology to commit human rights violations by tracking, and silencing, journalists, and activists (Wagner 2012, 7). Worse still, these technologies are sold by companies residing in places that consistently critique oppressive regimes for the very same human rights violations, such as North America and Europe (Wagner 2012, 7). This blatant disregard for human rights in cyberspace demonstrates the urgent need for new solutions to these new challenges.

This thesis will promote the use of the human security framework in cyberspace to address these new challenges. The conflict of interest between states and individuals in the physical and digital realms has shown that the current approach to security must be changed. By examining the dark side of the Internet, emerging technologies, and the problems they raise for human rights, this thesis will argue that human security must become the dominant paradigm in cyberspace.

CEU eTD Collection

1.3 Methodology

In order to highlight the need for a human security paradigm in cyberspace, this thesis will conduct a case study analysis of three companies discovered to be selling advanced censorship and

surveillance technology to oppressive regimes. These case studies have been chosen as they represent the extreme end of the failures of the traditional security paradigm in both the physical and digital realm. While these two realms are often considered siloed spaces where consequences remain within their respective borders, in reality the ramifications of actions in cyberspace reverberate through the physical realm and vice versa. Nowhere is this reality better exemplified than in the use of advanced censorship and surveillance technology to commit human rights violations.

Case-studies analysis was selected for this thesis, as it is the best methodological choice to explore the censorship and surveillance field. By utilizing case studies, it is possible to look at prominent examples over an extended period of time to illustrate the continued persistence of the problem. The Internet, and cyberspace in general, has grown rapidly over the past ten years, and these cases illustrate how the use of censorship and surveillance technology has grown with it. Additionally, because actions by states in cyberspace lack transparency, access to large swaths of data, or individuals willing to discuss the market, is extremely limited (Maurer 2016). Due to this challenge, much of the information about the market of advanced censorship and surveillance technology has come about from leaked internal documents or through the work of research/watchdog organizations such as the Citizen Lab at the University of Toronto. Finally, utilizing multiple case studies illustrates the geographic diversity of both the buyers and sellers of advanced censorship and surveillance technology. It is important to examine the use of this technology in multiple regions around the world as it highlights the pervasiveness of the problem.

The three case studies selected for this paper are Blue Coat Systems, Hacking Team, and Netsweeper. These three cybersecurity companies have been implicated in the selling of offensive and intrusive surveillance and censorship software at different times over the past ten years. These three cases were chosen for their status as influential cases, as well as their geographical and chronological spread. Influential case studies, according to John Gerring in *Case Selection for Case-*

CEU eTD Collection

Study Analysis: Qualitative and Quantitative Techniques, are cases that can either prove or disprove the rule, as well as potentially disconfirming or reconceptualizing a theory (Gerring 2008, 657). These three cases fill this role as they have come to define the rule of cybersecurity companies knowingly engaging in unethical behavior, and are among the few whose activities have been documented in great detail.

The first case study, Blue Coat Systems, in 2011 became one of the first and most prominent examples of a United States company selling technology used in human rights violations to Syria at the beginning of the Arab Spring (Aleaziz 2011a). Blue Coat Systems' technology was found to be used by the Assad regime to track and silence dissidents throughout Syria (Aleaziz 2011a). The second case deals with Hacking Team, an Italian company which in 2015 had 400 gigabytes (GB) of data leaked, shining a light onto the expanding zero-day exploit market and the continued practice of cybersecurity firms aiding repressive regimes in stifling dissent (Hern 2015). The final case, Netsweeper, a Canadian company that has long been accused of selling software to oppressive regimes, has recently come under intense scrutiny after a report by Citizen Lab found its censorship technology being used to censor information including, LGBTQI+, human rights, and sex education sites in multiple countries around the world (Deibert 2018).

While there are clear benefits to using case studies to highlight the pressing need for human security in cyberspace, there are limitations as well. First, the limited scope of this thesis makes it impossible to detail the complex technical nature and vast dealings of the companies involved in each case study. As such, prominent examples of each company's technologies have been selected for more detailed examination. The selection of examples within each case study, while necessary, means there is a level of authorial subjectivity in the information presented in this thesis. Additionally, subjectivity is also present in the selection of the three case studies as there have been many examples of cybersecurity firms selling advanced censorship and surveillance technology to oppressive regimes over the past ten years. The selection and designation of the three cases in this

CEU eTD Collection

thesis as influential is based on a personal understanding of the timing, coverage and context that defined each case. Lastly, the general lack of transparency and limited information about the use of advanced censorship and surveillance technology makes it difficult to extrapolate the findings of these case studies onto the entire censorship and surveillance field.

Even with the aforementioned limitations, these three cases accentuate the pressing need to change the security paradigm in cyberspace. Cybersecurity companies should be working to improve the security of individual users, not helping oppressive regimes commit human rights violations. Without human security in cyberspace, the Internet and emerging technologies will never fulfill their potential to strengthen human rights, but will remain powerful tools of oppression.

CEU eTD Collection

Chapter 2: Case Studies in Censorship, Surveillance, and Human Rights

Inalienable rights, such as the freedom of expression and the right to privacy are critical to the successful functioning of societies. The fight to protect these rights no longer resides solely in the physical realm, as the rapid emergence of cyberspace has drastically altered the way in which people access information and communicate. The three case studies selected for analysis, Blue Coat Systems, Hacking Team, and Netsweeper, all present important and unique examples of the distinct challenges to preserving people's basic human rights in the digital and physical realm. These companies are representative of an industry that has become willing to sacrifice the security of people in order to fulfill the desires of governments. As the world continues to rely more and more on the Internet, the ramifications of what happens in cyberspace have serious physical and potentially violent consequences for all.

From a technical standpoint, these case studies deal with what is termed as 'dual-use' technology. Censorship and surveillance technology is often considered to be dual-use technology because it can have both military and non-military purposes (Wagner 2012, 7). Conceptually, this term is also important as the technology itself is theoretically neutral, but how it is used drastically affects potential outcomes, from simple network monitoring to human rights violations (McCarthy 2010; Feenberg 2012, 264; Wagner 2012, 7; Wagner et al. 2015, 7; Deibert 2016). Broken down even further, this type of dual-use technology is considered to have two main categories: network traffic management and targeted device intrusion (Deibert 2016). Network traffic management includes content filtering and deep packet inspection (DPI) technology, and device intrusion typically entails malware utilizing zero-day exploits or similar tools to gain access to an individual's device (Deibert 2016). The ways in which these technologies were used will be more specifically outlined in each case study to provide examples and ramifications of dual-use technology in practice.

CEU eTD Collection

The three cases will be presented chronologically, based upon when their activities were first, or most prominently, discussed in the media. The first case study will examine the use of Blue Coat Systems technology in Syria at the beginning of the Arab Spring in 2011 (Aleaziz 2011a). Second, Hacking Team, an Italian company will be studied for its work with repressive governments around the world and blatant disregard for human rights concerns (Hern 2015). Finally, Netsweeper, a Canadian company, will be analyzed as its censorship software is currently being used in many countries with ongoing human rights crises to block access to legitimate information (Deibert 2018). The presentation of these cases will clearly demonstrate the ways in which cybersecurity technology is often actively eroding human rights, and why human security needs to become a defining feature of cyberspace. While many point to cybercrime and the detriment it is having on the world, it is these human rights violations committed by states with the help of cybersecurity firms in the North American and Europe that are creating the most insecurity in the digital and physical realms.

2.1 Blue Coat Systems: Censorship, Surveillance, and the Arab Spring

In 2011, as the Arab Spring was continuing to unfold, archives from fallen regimes exposed a market of European and North American cybersecurity companies selling advanced dual-use censorship and surveillance technology to oppressive regimes (Maurer 2016). It was during this time that equipment made by Blue Coat Systems, a cybersecurity firm based out of California in the U.S., was discovered to be operating in Syria under the Assad regime to stamp out dissent (Nachawati 2011). In addition to use in Syria, it was also uncovered that similar Blue Coat technology was being employed in multiple countries around the world including Burma[2], whose military junta was also well known for committing human rights violations (Dalek and Senft 2011).

[2] The Citizen Lab report cited in this sentence refers to the country Myanmar, as its former name Burma

CEU eTD Collection

At a time when democratic movements were sweeping much of the world, the technology developed by Blue Coat Systems, was helping to ensure they did not succeed.

Before the revelation that Blue Coat Systems' equipment was being used in Syria, there was already widespread consensus that the Syrian government was using advanced censorship and surveillance technology to track and silence dissidents (Staff 2011). As opposed to the successful and prolific use of social media in the uprisings in Tunisia and Egypt, activists in Syria were extremely wary of the information they would post online (Staff 2011). In early 2011, firsthand accounts began to emerge out of Syria that police forces were arresting, and imprisoning activists who posted anti-Assad comments online, and forcing many to hand over passwords to social media accounts (York 2011a; Preston 2011). It was clear, based on these people's interactions with security forces that they were being closely monitored and targeted online (Preston 2011). Then in October 2011, tech activist group Telecomix released 54 GB of log files, which showed that the Syrian Telecommunications Establishment had been using Blue Coat Systems' devices to filter and monitor Internet connections throughout Syria (Nachawati 2011). The logs revealed that the surveillance technology had been used to infiltrate nearly all personal communication online, including traffic that users believed was encrypted (Wagner 2012, 9). What these records made clear was that the DPI and content filtering technology provided by Blue Coat Systems had no legitimate use beyond violating people's privacy and freedom of expression.

Blue Coat Systems initially denied this report, as it was prohibited by U.S. sanctions and export controls to sell its equipment to Syria (Dalek and Senft 2011). However, following two weeks of media reports and investigative efforts, Blue Coat Systems admitted that the devices in question had been shipped to Dubai for use in Iraq, but unbeknownst to Blue Coat, had ended up in Syria (Aleaziz 2011b). Following Blue Coat's revelations, its Senior VP stated the company's desire to never sell products to embargoed countries, but in so doing failed to express any concern over human rights violations facilitated by its technology (York 2011b). This lack of regard for

CEU eTD Collection

human rights, illustrates the failing of corporate social responsibility, and cybersecurity firms willingness to facilitate human rights violations when it is not illegal. Highlighting this fact, Blue Coat Systems did not stop selling its products to oppressive regimes. A 2013 report by Citizen Lab found their censorship and surveillance technology being used in countries with poor human rights records, such as, Bahrain, the UAE, Saudi Arabia, Egypt, Sudan, Malaysia, Russia and Venezuela to name a few (Marquis-Boire et al. 2013). This case exemplifies the states able to control people's lives with the help of cybersecurity firms when human security is not the primary objective in cyberspace.

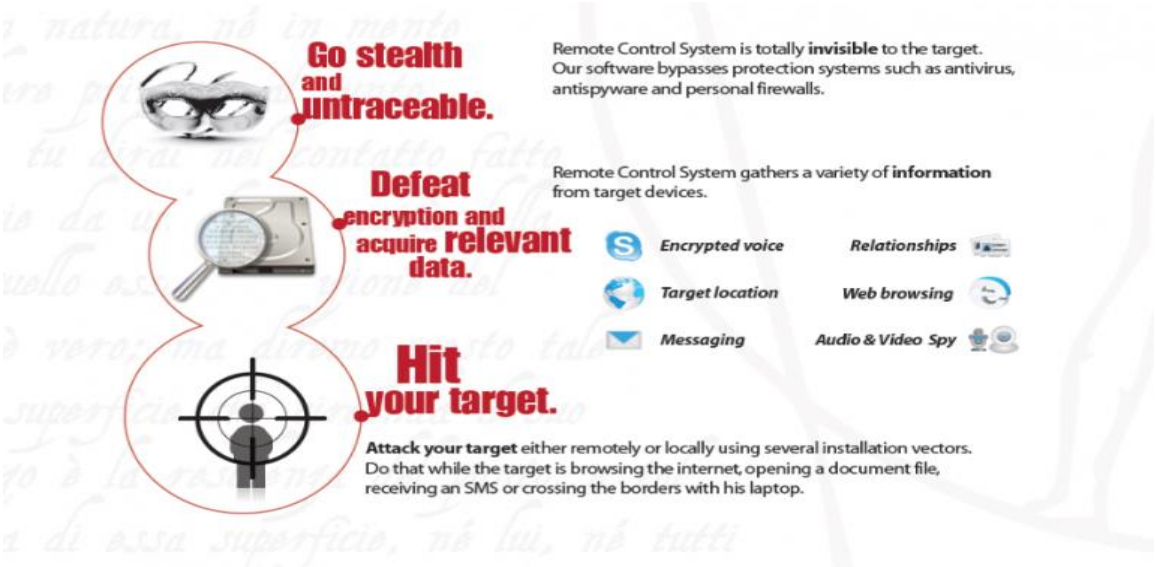
2.2 Hacking Team

In 2015, four years after the Blue Coat Systems revelations, information about the scope and inner workings of the censorship and surveillance industry remained mostly obfuscated. Then in July of that year, the cybersecurity/espionage company, Hacking Team, was itself hacked and 400 GB of its internal documents released (Captain 2015). The hack, among other things, provided a fresh snapshot of the zero-day exploit market, its inner workings, and pricing (Zetter et al. 2015). Internal and external Hacking Team communications highlighted the growing scope of the market, with zero-day exploits ranging in price anywhere from USD $30,000 to USD $500,000 (Zetter et al. 2015). Additionally, the leak confirmed multiple Citizen Lab reports pertaining to Hacking Team's software's nefarious uses, from targeting Ethiopian journalists, to its use in places such as Saudi Arabia, Sudan, Azerbaijan, Kazakhstan and Uzbekistan (Marczak et al. 2014b). These revelations provide yet another example of the willful disregard for human security in cyberspace.

Hacking Team first came under scrutiny in 2012, when Citizen Lab, published an in-depth report on the use of the company's Remote Control System (RCS), a device intrusion system, to infiltrate the computers of human rights activists in the UAE, and a civil society group in Morocco (Singh 2015). See in figure 1 below, a section of a leaked brochure from Hacking Team in 2011, detailing the RCS system (Marczak et al. 2014a; "WikiLeaks - The Spy Files" n.d.).

CEU eTD Collection

Figure 1. Hacking Team Brochure



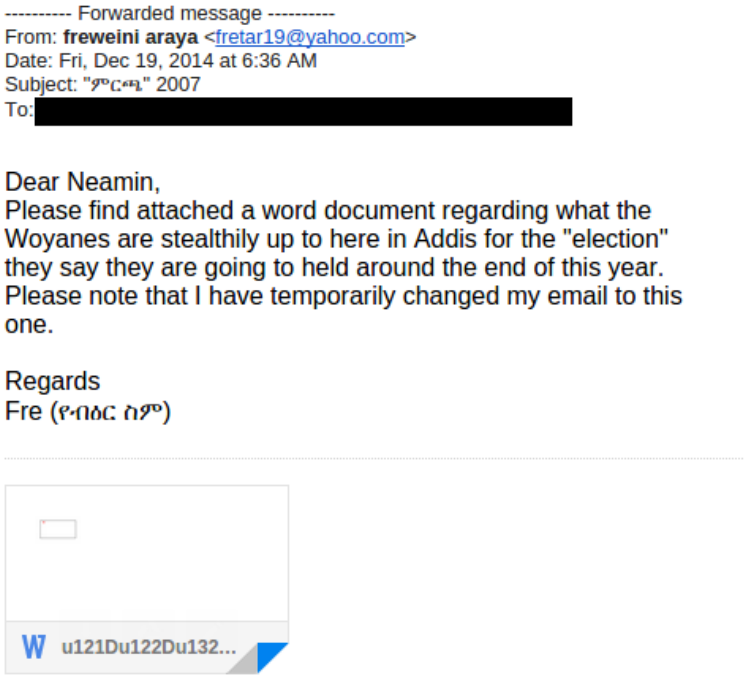
The brochure emphasizes Hacking Team's ability to stealthily hit specific targets and defeat device encryption to access all desired data. In addition to advertising themselves as capable of bypassing antivirus software, Hacking Team chose to highlight their ability to remotely spy on targets via devices' audio and video components, as well as to gather information pertaining to a target's relationships with other individuals. A common method employed by Hacking Team and others to infiltrate a target's device is social engineering, a tactic that attempts to manipulate people into clicking links or granting access to their accounts by actors impersonating a trusted source or individual (Hulme and Goodchild 2017; Marquis-Boire 2012). While there are legitimate and lawful reasons for security forces to track certain people, a Citizen Lab report found that Hacking Team's software was often used to target political adversaries and not security risks (Marczak et al. 2014b).

A prime example of the unethical political use of Hacking Team's technology was demonstrated in its use by the Ethiopian government. In 2013, the Ethiopian government, with the help of Hacking Team used its RCS to infect personal computers and monitor Ethiopian journalists operating in the diaspora (Marczak et al. 2014a). Specifically, the software was used to target Ethiopians working for Ethiopian Satellite Television Service (ESAT), an opposition media outlet, operating out of the Washington D.C. area (Marczak et al. 2014a). Beyond just monitoring

CEU eTD Collection

individuals in the diaspora, Ethiopia also clamped down on journalists within its borders, trailing only Eritrea in the jailing of journalists between 1993 and 2013 (*Committee to Protect Journalists* 2013). Ethiopia's track record alone should have been enough to halt all sales to the country, considering Hacking Team claimed at the time that it, "...goes to great lengths to assure that our software is not sold to governments that are blacklisted by the EU, the USA, NATO and similar international organizations or any 'repressive regime (Hern 2015)." However, even following the public release of the malicious uses of its software by Ethiopia in 2013, a year later in 2014, it was uncovered that Hacking Team was still supporting the Ethiopian government's attempts to infiltrate opposition systems. See the social engineering attempt to infiltrate the Managing Director of ESAT's computer, in figure 2 below, from Citizen Lab's 2015 report on the situation (Marczak, Scott-Railton, and McKune 2015).

Figure 2. Email with Spyware Sent to the Managing Director of ESAT



These examples of Hacking Team's continued support of the Ethiopian government's attempt to target political opponents around the world exemplify the company's complete disregard for human rights. Even after repeatedly denying their involvement with repressive

CEU eTD Collection

regimes, the 400GB data leak confirmed much of what had been reported by Citizen Lab and other groups. From Ethiopia to Sudan, Bahrain and Uzbekistan, Hacking Team facilitated human rights violations around the world (Hern 2015). Unfortunately, as Citizen Lab Director, Ron Deibert, noted to the Toronto Star, "Hacking Team is a symptom of a larger disease (Singh 2015)." The actions of Hacking Team demonstrate the failings of the traditional security paradigm in cyberspace. When organizations are willing to advertise their products for use by law enforcement, all the while knowing their technology is being used by oppressive regimes to commit human rights violations, they are clearly not interested in protecting the individual. Human security demands individuals have political, personal, and community security, all of which are explicitly violated by organizations such as Hacking Team.

2.3 Netsweeper

The final company and its activities that will be examined in this paper is Netsweeper. Netsweeper is a Canadian Internet filtering company based out of Waterloo, Ontario (Dalek et al. 2018b). Netsweeper and its technologies uses have been scrutinized previously; however, a March 2018 report by the Citizen Lab, *Planet Netsweeper*, provided an extremely comprehensive look into Netsweeper's global activities (Dalek et al. 2018b). As opposed to the device intrusions systems detailed in the Hacking Team case study, the investigation into Netsweeper found a number of troubling applications of its content filtering technologies, with serious human rights implications. Netsweeper technology was found to be operational in over 30 countries, including being used to filter content on a national level in Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, UAE, and Yemen (Dalek et al. 2018b). Amongst its many uses, it was found to be blocking religious content in Bahrain and political information in the UAE (Dalek et al. 2018b). Furthermore, Citizen Lab found that the technology was purposely miscategorizing sites pertaining to issues such as LGBTQI+ identities, and HIV/AIDS prevention, as pornographic so that they would be blocked (Dalek et al. 2018b). Unfortunately, these human rights violations are not the

CEU eTD Collection

worst facilitated by Netsweeper technology. Its current use in the war in Yemen exemplifies the ways in which censorship technology can greatly contribute to instability and physical violence.

Yemen has been engaged in a civil war since 2015 that has left 75 percent of its population, or 22.2 million people, in need of humanitarian or protection assistance ("In Focus: Yemen" 2018). As the war drags on, the world's worst humanitarian crisis (Guterres 2018) will only continue to worsen. It is with this context in mind that we approach the role Netsweeper technology is playing in this crisis. Before the outbreak of the war, Netsweeper technology was already being used by the government on the Internet service provider (ISP), Yemennet, to censor political content and independent media (Dalek et al. 2018a). Following the rebel Houthi's capture of Yemen's capital Sana'a and the country's communication infrastructure, the Houthi's broadened the scope of filtering practices to include many local and regional news websites (Dalek et al. 2018a). Media organization, Sahafa.net, has publicly pleaded with Netsweeper to discontinue its services in Yemen as they claim its technology is being used for military purposes by the Houthis (Dalek et al. 2018a). This plea came at the same time that a *New York Times* report found that Houthi's had been using their control over telecommunications infrastructure to shut down the Internet for days at a time, and block sites that their enemies could be using to communicate (Hubbard and Youssef 2017; Dalek et al. 2018a). This means that Netsweeper technology is being used for military purposes in a war in which both parties have been accused of human rights violations, including war crimes against children, and is preventing Yemenis from accessing potentially lifesaving information pertaining to the war (Dalek et al. 2018a; United Nations Security Council 2017, 2).

While the war in Yemen may not be as well covered by the media as the war in Syria, the massive humanitarian crisis occurring there is no secret. By continuing to provide Internet filtering services, Netsweeper has taken an active role in the war in Yemen. Netsweeper has knowingly facilitated freedom of expression infringements in a war that has left 22.2 million people in need

CEU eTD Collection

of protection and humanitarian assistance. In siding with military forces, Netsweeper has played a large role in the erosion of human security for everyone living in Yemen.

CEU eTD Collection

Chapter 3: Analysis and Recommendations

How the world responds to the changes brought about by the Internet has enormous ramifications for the future of human rights. The examples of Blue Coat Systems, Hacking Team, and Netsweeper underscore the potentially fatal consequences of ignoring these rights in cyberspace. In order to protect and promote human rights in the physical and digital realm, the security paradigm of cyberspace must transition from a traditional to human-centric approach. With human security providing the theoretical framework for a new approach to cybersecurity, the world will take a critical step forward in ensuring human security for all. To help bring about this reality, this chapter will outline the core conceptual areas of human security that must be protected in cyberspace based upon a detailed analysis of the case studies from Chapter 2. Additionally, this analysis will provide the framework for recommendations of policies and practices needed to ensure human security in cyberspace. Improved encryption practices, the elimination of backdoors, and increased transparency, to name a few, are all necessary components of human security in cyberspace. While these recommendations are critical to ensuring human security in cyberspace today, what is most important is that moving forward the theoretical framework of human security drive all policies and laws pertaining to cyberspace.

3.1 Borderless Rights and Ramifications

3.1.1 Community and Political Security in the Digital and Physical Realms

Two aspects of human security as laid out in the 1994 HDR, community and political security have considerable overlaps and are crucial to the successful implementation of human security in cyberspace. As discussed in Chapter 1, political security mandates people live in a society where their human rights are protected, such as freedom of expression and freedom of assembly (UNDP 1994, 32). Community security adds to this by requiring individuals be protected from

CEU eTD Collection

exploitative practices within communities, as well as being free from discrimination due to affiliation with a certain group (UNDP 1994, 30,31). In cyberspace the protection of these two aspects of human security have often been willfully ignored, at best, by states and cybersecurity firms alike as they have sought technological advancement and state security over all else.

The case studies presented in Chapter 2, of Blue Coat Systems, Hacking Team, and Netsweeper, illustrate the direct conflict between states and these two aspects of human security. In Syria, Ethiopia, and Yemen, the advanced censorship and surveillance technologies employed by these states was typically used to specifically target certain groups and individuals based upon their political and community affiliations. In Syria, Blue Coat Systems technology was used to individually target and silence dissidents within the country (Staff 2011; Dalek and Senft 2011). Similarly, in Ethiopia, surveillance technology deployed by Hacking Team was also used to target journalists, particularly those with connections to opposition groups (Marczak et al. 2014a; "Ethiopia: Hacking Team Lax on Evidence of Abuse" 2015). These two violations of community and political security highlight the unethical and political uses of intrusive cybersecurity technology by states that greatly limit freedom of expression and freedom from discrimination.

The case of Netsweeper produces similar results from a slightly different use of the technology that was employed in the cases of Blue Coat Systems and Hacking Team. As opposed to the use of targeted device intrusion technology, the censoring and filtering systems deployed on Yemennet have been used as a weapon of war to block access to information pertaining to military activities (Dalek et al. 2018a). Additionally Netsweeper technology has been found to be used to censor legitimate information pertaining to the LGBTQI+ community and reproductive health in multiple countries (Dalek et al. 2018b). Targeting groups such as the LGBTQI+ community, and HIV/AIDS patients', freedom of expression is a discriminatory practice that places a severe limit on individuals' ability to access pertinent and necessary information. The ways in which

CEU eTD Collection

Netsweeper's technology is used in Yemen illustrates how violations of freedom from discrimination and freedom of expression in cyberspace can lead to sustained insecurity for all.

The case studies in Chapter 2 make clear that the need to protect political and community security is just as important in cyberspace as it is in the physical realm. Unfortunately, as indicated in Chapter 1, once the security of one aspect of human security is compromised, so too are others. As such, the failure to protect political and community security in cyberspace, puts individual personal security at risk.

3.1.2 Physical Consequences from a Digital World

Personal security, or the protection from physical violence, at first glance seems to not have direct application in cyberspace. Unfortunately, however, the case studies from Chapter 2 epitomize how dependent one's physical security can be upon their overall security in cyberspace. By denying people the right to political and community security, states employing advanced censorship and surveillance software, were able to leverage activities in cyberspace into having violent physical ramifications. In Ethiopia, the remote infiltration of personal devices used to track and arrest journalists and activists has had a chilling effect on freedom of expression in the country due to legitimate threats to their personal security (Watch 2014). In Yemen and Syria, the uses of censorship and surveillance technology for military purposes at a time of war places citizens directly in harm's way as an inability to access pertinent information limits one's ability to make life saving decisions (Dalek et al. 2018a; Aleaziz 2011a). These instances of censoring and surveilling targeted individuals at times of war, and political unrest, emphasizes the negative physical results that arise from a failure to ensure human security in cyberspace.

What is also highly disconcerting about these cases is the responses from the companies after their products were discovered to be facilitating human rights violations. At the beginning of the unrest in Syria, it was well known that Assad was violently cracking down on all forms of dissent (Staff 2011). Included in this crackdown were threats, physical attacks and the detention

CEU eTD Collection

of many journalists and bloggers ("Detained Bloggers and Journalists in Syria: The List Gets Longer" 2011). Whether or not it can be believed that Blue Coat Systems had no knowledge of the fact that their technology was being used in Syria, their public response to this discovery showed no remorse for the direct attacks on human security that their technology facilitated (York 2011b). Additionally, after this incident, Blue Coat Systems continued to sell technology to countries with poor human rights records (Marquis-Boire et al. 2013). This disregard for human rights shows just how little regard for human security exists in cyberspace today.

Unfortunately, the case of Hacking Team shows that Blue Coat Systems' disregard for human rights may typify the field. After Citizen Lab discovered that Hacking Team's technology was being used by the Ethiopian government to track journalists in the diaspora in 2013, they did not end their relationship with the government but chose to continue to support its efforts (Marczak, Scott-Railton, and McKune 2015). This comes after Hacking Team had publicly stated that it made every effort to ensure their software was not used by repressive or blacklisted regimes (Hern 2015). The public face put up by Hacking Team, contrasted with the reality of its operations that were exposed by the 400GB data leak, exemplifies how even when homage is paid to human rights, human security is never a priority.

Lastly, the case of Netsweeper raises similar concerns with its use in Yemen during a known civil war. The war, which has led to a devastating human rights crisis in the country, has seen Netsweeper technology used as a tool of war by the military (Hubbard and Youssef 2017). Media organizations within Yemen have even made public appeals to Netsweeper to end its contract with Yemennet, as it was being used to commit human rights violations (Dalek et al. 2018a). The silence from Netsweeper in response to these allegations is equally as telling as the lack of remorse seen in the case of Blue Coat Systems.

All of these cases show that the traditional approach to security in cyberspace, which places the security of the state over the individual, can have serious negative repercussions. The physical

CEU eTD Collection

harm that was enabled by advance censorship and surveillance technology in Syria, Ethiopia, and Yemen, makes it clear that the consequences of actions in cyberspace do not stay within its borders. Beyond a failure to merely protect human security online, these cases show that cybersecurity firms are actually helping to attack it. As the Internet continues to become more and more intertwined with our daily lives, the need to move to a human security paradigm in cyberspace is critical to ensure the protection of human rights. Without political, community, and personal security protected in cyberspace, the Internet will continue to be a favorite tool of oppressors. In order to transition away from this dark reality, a concerted effort must be made to put human security at the center of policy and practice in cyberspace.

3.2 Recommendations

The conceptual need to place political, community, and personal security at the forefront of cybersecurity has been made evident by the case studies presented in Chapter 2. Once this rationale behind the move to human security is understood, the challenge then becomes deciding how to move from a conceptual framework to practical implementations. The first step in this process is to focus on the human rights that undergird political, community, and practical security in cyberspace: the right to privacy, freedom of expression, freedom of assembly, and freedom from discrimination. As the Internet and digital world continue to evolve, an emphasis on these human rights is paramount to the success of the human security framework in cyberspace. Vital to protecting these rights and aspects of human security is to work to remove unnecessary vulnerabilities in the system. By improving and expanding encryption standards, ending mass surveillance practices, increasing transparency, protecting anonymity and ensuring the integrity of people's data online, great strides can be made in protecting and promoting human security in the physical and digital realms.

CEU eTD Collection

3.2.1 Human Cybersecurity in Practice

In Myriam Dunn Cavelty's paper, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", she states that both a strategically insecure cyberspace filled with vulnerabilities and a secure and resilient cyberspace cannot coexist (Dunn Cavelty 2014, 11). This means that while intelligence agencies may desire a cyberspace designed to have vulnerabilities, as seen in the Apple versus FBI case presented in Chapter 1, these vulnerabilities lead to a weakened system for all. Key to reducing vulnerabilities and protecting the system is to expand the use of encryption and eliminate backdoors (Roth 2017).

Ensuring that communications and information are encrypted helps to keep unwanted eyes from personal and sensitive data (Grimes 2017). Encryption greatly improves human security in cyberspace in multiple ways. The decreased ability of outside actors to access personal information and communications protects the integrity of data in cyberspace and subsequently reduces individual vulnerability to cybercrime, cyber-espionage and mass surveillance (Dunn Cavelty 2014, 11; Roth 2017). By protecting individuals from these vectors of information gathering, people can have more trust in the integrity of their personal information and communications. The added trust strengthens freedom of expression and reduces the possibility of discrimination online, as individuals will be more willing to share dissenting political opinions and associate with potentially ostracized communities. The benefits seen here also illustrate the importance of anonymity online. If everyone were forced to identify themselves online, it would have a tremendous stifling effect on political dissident, activism, and whistleblowing. These are necessary components of freedom of expression, freedom of assembly and freedom from discrimination that must be protected. Additionally, as mentioned in Chapter 1, human security demands an integrative and active approach where security does not merely respond to crises but is proactive in their prevention. Improving the security of communications and anonymity online

CEU eTD Collection

is a proactive measure in the defense human rights, which is central to the concept of human security.

It must be noted however, that there are many serious negative externalities that arise from these protections, such as technology facilitated violence against women (TFVAW), and general hate speech online. While these are grave problems, their solutions must be addressed within the human security framework of cyberspace currently being outlined. The inability to identify perpetrators of TFVAW in cyberspace due to strong anonymity is highly disconcerting, however, the consequences of granting law enforcement, or other state-based actors, this ability has been shown to be grave. As seen in the cases of Syria, Ethiopia, and Yemen, when governments have the ability to easily identify all actors in cyberspace, human rights such as freedom of expression and freedom from discrimination suffer. Solutions to this problem go beyond the scope of this thesis, but are an essential area for future research that should be conducted simultaneously with the creation of human security based policies for cyberspace.

Beyond the negative externalities mentioned above, the continued call for backdoors into encryption standards by states is highly problematic (Roth 2017). States argue that backdoors are needed in order to monitor and arrest criminals communicating online, however, the creation of a backdoors would not merely weaken the system for criminals, but would entail reduced security for all (Dunn Cavelty 2014, 10). A major area of concern that arises from the creation of a backdoor for an encryption standard is the inability to guarantee only law enforcement officials are able to access it, leaving it open for potential exploitation by malevolent actors (Dunn Cavelty 2014, 10). Additionally, the examples of Syria, Ethiopia, and Yemen in Chapter 3, show that the seemingly benign intent of law enforcement and intelligence agencies cannot always be taken at face value. The state's ability to surveil people and censor information at will has been shown to have dire consequences for the protection of human rights. As such, it is crucial for the protection

CEU eTD Collection

of human security online that backdoors are not created for states. When civil liberties are sacrificed in the name of security, individual lives are left far more insecure.

Two remaining challenges made evident by this thesis are the zero-day market and the general lack of transparency in cyberspace. The entry of states into the zero-day market, where unknown security vulnerabilities in software are sold, has drastically increased its size and driven up prices (Dunn Cavelty 2014, 8). Combine this with a lack of transparency and regulation, and the security risks for individuals are significant. So long as vulnerabilities that potentially affect millions of people are used to spy on people or in offensive cyberweapons, human security will never be realized in cyberspace. Furthermore, an increase in general transparency in cyberspace is needed to provide a check on state's power and actions (Deibert 2012, 274). Reducing the risk of escalation in cyberspace and allowing citizens and states to provide checks on each other's actions will lead to a more stable cyberspace. Unfortunately, these two recommendations have serious practical limitations. The lack of transparency in cyberspace is coveted by states. Transparency helps states to obfuscate their actions among the activities of cybercriminals, as seen in the case of the Stuxnet virus (Deibert 2012, 268). So long as the traditional security paradigm in cyberspace continues to allow for enough insecurity to hide states' activities it will be very difficult to advance a human security framework. Thus for transparency to become a prominent part of cyberspace a push must be made to change governmental attitudes and posturing in cyberspace.

Even though there are serious obstacle to implementing human security in cyberspace, a framework built around political, community, and personal security will provide a solid foundation for its implementation. The practical steps and concepts pertaining to human security in cyberspace detailed in this section are critical starting points for ensuring the protection of human rights and integrity. The case studies of Blue Coat Systems, Hacking Team, and Netsweeper have shown that until human security becomes the dominant paradigm in cyberspace it will never be realized in the physical realm.

CEU eTD Collection

Conclusion

How the world chooses to approach the concept of security has enormous ramifications for its policies and beneficiaries. As the digital age continues to connect more of the world, the conceptualization of security in cyberspace is having a growing impact on individuals' physical security. This thesis has made evident that the traditional approach to security, which places the integrity of the state above all else, has repeatedly resulted in greater insecurity for individuals. The cases analyzed in this thesis, Blue Coat Systems, Hacking Team, and Netsweeper, have illustrated that the current approach to cybersecurity is not only failing to protect individuals but is actively attacking their security. In order to address this problem, this thesis has sought to provide a methodological approach to the implementation of a human security paradigm in cyberspace and answer why it would better protect individuals than the current traditional security paradigm.

In taking the concept of human security beyond "freedom from fear" and "freedom from want", the 1994 Human Development Report illustrated how from poverty to disease, to natural disasters and war, protection from violent external aggression was not the only thing required to keep individuals secure (UNDP 1994, 23). While in 1994 the Internet's commercial roots were just beginning, the massive digital revolution that has taken place since has created a need to implement these same concepts of human security in cyberspace. No longer is a reactive approach to security, designed to protect the integrity of the state, acceptable for the protection of individuals. Instead, a proactive approach that recognizes the interdependence of the many facets of people's lives is needed to ensure security benefits all and promotes human rights.

The examples of Blue Coat Systems, Hacking Team, and Netsweeper, illustrated how severe the negative ramifications can be when human security is not protected in cyberspace. The expanding market of cybersecurity firms willing to be complicit in the human rights violations of oppressive regimes exemplifies the failed priorities of the traditional security paradigm in cyberspace. The use of advanced censorship and surveillance technology to crack down on dissent

CEU eTD Collection

and control access to information is antithetical to the human security paradigm. Human security demands human rights be actively protected, including the freedom of expression and freedom from discrimination, core tenets of political and community security, be actively protected.

With the understanding from the case studies that actions in cyberspace do not stay within its borders, it is critical that human security be protected in cyberspace for it to be fully realized. This cross contamination clearly illustrates that the interdependence that defines human security in the physical realm is replicated in cyberspace. As such, this thesis has made basic recommendations including the expanded use of encryption, elimination of backdoors, protecting anonymity, and increased transparency, in order to better protect the pillars of human security online.

What is most important, however, is that future policies pertaining to security in cyberspace are devised based upon the conceptual framework of human security. Both individuals and states will benefit from an implementation of human security in cyberspace as a more secure cyberspace will help to keep society functioning. Human rights, such as freedom of expression, freedom from discrimination and the right to privacy, are all necessary to keep society evolving and power in check. By utilizing the conceptual framework of human security in cyberspace, security that is relevant for individuals will help to ensure cyberspace positively impacts the world.

CEU eTD Collection

Reference List

Aleaziz, Hamed. 2011a. "Syria Uses US Technology in Cyber Crackdown." *Mother Jones*, October 19, 2011. https://www.motherjones.com/politics/2011/10/blue-coat-systems-internet-blocking-syria/.

———. 2011b. "After MoJo Investigation, US Company Admits Its Technology Used in Syria." *Mother Jones*, October 31, 2011. https://www.motherjones.com/politics/2011/10/blue-coat-admits-syria-connection/.

Attina, Fulvio. 2016. "Traditional Security Issues." In *China, the European Union, and the International Politics of Global Governance*, edited by J. Wang and W. Song, 175–93. Palgrave Macmillan, New York.

Bajpai, Kanti P. 2000. *Human Security: Concept and Measurement*. University of Notre Dame, Joan B. Kroc Institute for International Peace Studies.

Captain, Sean. 2015. "Nothing Is Untraceable: How The HackingTeam Got Busted [UPDATED]." Fast Company. Fast Company. July 6, 2015. https://www.fastcompany.com/3048280/nothing-is-untraceable-how-the-hacking-team-got-busted.

Cardozo, Nate, and Andrew Crocker. 2018. "The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, But Leadership Didn't Say That." Electronic Frontier Foundation. April 2, 2018. https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say.

Chiarello, Leonir. 2015. "The Emergence and Evolution of the Concepts of Human Rights and Human Security." *The Center for Migration Studies of New York (CMS)*, October. http://cmsny.org/publications/chiarello-human-rights-and-human-security/.

Committee to Protect Journalists. 2013. "Ethiopia Arrests 2 Journalists from Independent Paper," November 5, 2013. https://cpj.org/2013/11/ethiopia-arrests-2-journalists-from-independent-pa.php.

Dalek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. 2018a. "Planet Netsweeper: Country Case Studies." The Citizen Lab. April 25, 2018. https://citizenlab.ca/2018/04/planet-netsweeper-section-2-country-case-studies/.

———. 2018b. "Planet Netsweeper: Executive Summary." The Citizen Lab. April 25, 2018. https://citizenlab.ca/2018/04/planet-netsweeper/.

Dalek, Jakub, and Adam Senft. 2011. "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma - The Citizen Lab." The Citizen Lab. November 9, 2011. https://citizenlab.ca/2011/11/behind-blue-coat/.

Deibert, Ronald. 2012. "Growing Dark Side of Cyberspace (... and What to Do about It)." *Penn St. JL & Int'l Aff.* 1. HeinOnline: xiii.

———. 2016. "What to Do about 'Dual Use' Digital Technologies?," November 29, 2016. https://deibert.citizenlab.ca/2016/11/dual-use/.

———. 2018. "Sweeping the Internet for Netsweeper," April 25, 2018. https://deibert.citizenlab.ca/2018/04/planet-netsweeper/.

"Detained Bloggers and Journalists in Syria: The List Gets Longer." 2011. Global Voices Advocacy. October 28, 2011. https://advox.globalvoices.org/2011/10/28/detained-bloggers-and-journalists-in-syria-the-list-gets-longer/.

Dunn Cavelty, Myriam. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20 (3): 701–15.

"Ethiopia: Hacking Team Lax on Evidence of Abuse." 2015. Human Rights Watch. August 13, 2015. https://www.hrw.org/news/2015/08/13/ethiopia-hacking-team-lax-evidence-abuse.

Feenberg, Andrew. 2012. *Questioning Technology*. Routledge.

Gerring, John. 2008. "Case Selection for Case-Study Analysis: Qualitative and Quantitative Techniques." In *The Oxford Handbook of Political Methodology*, edited by Janet M. Box-Steffensmeier, Henry E. Brady, and David Collier. Oxford University Press.

Gomez, Oscar A., and Des Gasper. n.d. "Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams." UNDP. http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf.

Grimes, Roger A. 2017. "Why We Need to Encrypt Everything." CSO Online. April 11, 2017. https://www.csoonline.com/article/3188865/data-protection/why-we-need-to-encrypt-everything.html.

CEU eTD Collection

Guterres, Secretary-General Antonio. 2018. "Secretary-General's Remarks to the Pledging Conference on Yemen [as Delivered] | United Nations Secretary-General." Geneva, Switzerland, April 3. https://www.un.org/sg/en/content/sg/statement/2018-04-03/secretary-generals-remarks-pledging-conference-yemen-delivered.

Hern, Alex. 2015. "Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim." *The Guardian*, July 6, 2015. http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

Hubbard, Ben, and Nour Youssef. 2017. "Yemen's War Enters a Dark Stage as Rebels Squeeze the Capital." *The New York Times*, December 23, 2017. https://www.nytimes.com/2017/12/23/world/middleeast/yemen-sana-houthis-saudi-arabia.html.

Hulme, George V., and Joan Goodchild. 2017. "What Is Social Engineering? How Criminals Take Advantage of Human Behavior." CSO Online. August 3, 2017. https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html.

"Human Security: A Stronger Framework for a More Secure Future | Human Development Reports." n.d. Accessed April 15, 2018. http://hdr.undp.org/en/content/human-security-stronger-framework-more-secure-future.

"In Focus: Yemen." 2018. UN News. March 5, 2018. https://news.un.org/en/focus/yemen.

"Internet Growth Statistics 1995 to 2017 - the Global Village Online." n.d. Accessed May 22, 2018. https://www.internetworldstats.com/emarketing.htm.

Kharpal, Arjun, and Kristina Roth. 2016. "Apple vs FBI: All You Need to Know." CNBC. CNBC. March 29, 2016. https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

Kovacs, Anja, and Dixie Hawtin. 2013. "Cyber Security, Cyber Surveillance and Online Human Rights." In *Stockholm Internet Forum*.

Liotta, Peter H., and Taylor Owen. 2006. "Why Human Security." *Whitehead J. Dipl. & Int'l Rel.* 7. HeinOnline: 37.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. 2014a. "Hacking Team and the Targeting of Ethiopian Journalists." The Citizen Lab. February 12, 2014. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

———. 2014b. "Mapping Hacking Team's 'Untraceable' Spyware." The Citizen Lab. February 17, 2014. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Marczak, Bill, John Scott-Railton, and Sarah McKune. 2015. "Hacking Team Reloaded." The Citizen Lab. March 9, 2015. https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Marquis-Boire, Morgan. 2012. "Backdoors Are Forever: Hacking Team and the Targeting of Dissent." The Citizen Lab. October 10, 2012. https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/.

Marquis-Boire, Morgan, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. 2013. "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools." The Citizen Lab. January 15, 2013. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

Maurer, Tim. 2016. "Internet Freedom and Export Controls." Carnegie Endowment for International Peace. Carnegie Endowment for International Peace. March 3, 2016. http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961.

McCarthy, D. R. 2010. "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet." *Foreign Policy Analysis*. academic.oup.com. https://academic.oup.com/fpa/article-abstract/7/1/89/1796108.

Nachawati, Leila. 2011. "BlueCoat: US Technology Surveilling Syrian Citizens Online." *Global Voices Advocacy*, October 10, 2011. https://advox.globalvoices.org/2011/10/10/bluecoat-us-technology-surveilling-syrian-citizens-online/.

Preston, Jennifer. 2011. "Syria Cracks Down on Social Media." *The New York Times*, May 22, 2011. https://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.

Reitman, Rainey. 2016. "3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance." Electronic Frontier Foundation. June 5, 2016. https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

CEU eTD Collection

Roth, Kenneth. 2017. "The Battle over Encryption and What It Means for Our Privacy." *Human Rights Watch*, June 28, 2017. https://www.hrw.org/news/2017/06/28/battle-over-encryption-and-what-it-means-our-privacy.

Selyukh, Alina. 2016. "A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?" *NPR*, December 3, 2016. https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

Singh, Amitpal. 2015. "Hacking Team Leak Highlights Citizen Lab Research." The Citizen Lab. August 6, 2015. https://citizenlab.ca/2015/08/hacking-team-leak-highlights-citizen-lab-research/.

Staff, Reuters. 2011. "Social Media: A Double-Edged Sword in Syria." *Reuters*, July 13, 2011. https://www.reuters.com/article/us-syria-social-media/social-media-a-double-edged-sword-in-syria-idUSTRE76C3DB20110713.

Taylor, Owen. 2004. "Challenges and Opportunities for Defining and Measuring Human Security." In *Disarmament Forum*, 14–24.

UNDP. 1994. "Human Development Report 1994." United Nations Development Program. https://market.android.com/details?id=book-pSa5Zrg5TnEC.

UNGA. 2016. "The Promotion, Protection and Enjoyment of Human Rights on the Internet." *United Nations General Assembly*.

United Nations Security Council. 2017. "Children and Armed Conflict." A/72/361-S/2017/821. United Nations Security Council. http://www.un.org/ga/search/view_doc.asp?symbol=A/72/361&Lang=E&Area=UNDOC.

Wagner, Ben. 2012. "Exporting Censorship And Surveillance Technology." Human Institute for Co-operation with Developing Countries. https://www.hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf.

Wagner, Ben, Joanna Bronowicka, Cathleen Berger, and Thomas Behrndt. 2015. *Surveillance and Censorship: The Impact of Technologies on Human Rights*. Publications Office.

Watch, Human Rights. 2014. "'They Know Everything We Do': Telecom and Internet Surveillance in Ethiopia." Human Rights Watch.

"WikiLeaks - The Spy Files." n.d. Accessed May 30, 2018. https://wikileaks.org/spyfiles/docs/hackingteam/147_remote-control-system.html.

York, Jillian C. 2011a. "The Dark Side of the Syrian Internet." *Index on Censorship*, June 1, 2011. https://www.indexoncensorship.org/2011/06/the-dark-side-of-the-syrian-internet/.

———. 2011b. "Blue Coat: Concern for Criminal Penalties, Not Human Rights." Electronic Frontier Foundation. October 29, 2011. https://www.eff.org/deeplinks/2011/10/blue-coat-acknowledges-syrian-government-use-its-products.

Zetter, Kim. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 11, 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Zetter, Kim, Kim Zetter, Lily Hay Newman, Garrett M. Graff, Lily Hay Newman, Lily Hay Newman, Andy Greenberg, and Louise Matsakis. 2015. "Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work." *Wired*, July 24, 2015. https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/.

CEU eTD Collection